RELEASE NOTES 3.5

Industry Interactive Procurement System (IIPS)

Numerous changes have occurred in the Industry Interactive Procurement System that affects all users. Below is a list of the Cyber Security requirements in the redesign of IIPS through the latest version 3.5, released August 30, 2004. Additional enhancements were also added to continue making IIPS user friendly. Items are listed in no particular order.

CYBER SECURITY REQUIREMENTS

LABELING FOR SENSITIVITY

A banner has been added to various documents in IIPS that may contain sensitive information. Though solicitation information is primarily for the general public, the purpose of the banner is to remind users that the information they may be viewing should be held in confidence. Those documents that include the banner are the Opportunity documents, Solicitation Document (Synopsis Modification/Solicitation Amendment), Solicitation Message, Application/Proposal Cover Page and Attachment Pages, Government Response (Negotiation/Clarification), Contractor Response, and Question/Answer pages. The banner is located at the top of each page.

RULES OF BEHAVIOR

A new web page has been added to inform all users of the general behaviors and intended use of the IIPS and Simplified Acquisition systems. The Rules of Behavior addresses information such as user types, user access, and individual accountability. A link to Rules of Behavior can be found at the e-Center home page, both IIPS and Simplified Acquisitions registration pages, and the Login page.

AUTOMATE REMOVAL OF OLD ACCOUNTS

In order to automate the removal of inactive accounts, the system has been designed to track a user's last login date and time. Once two years have passed since the last login, the user account will be removed from the system. If a user's account has been removed, the user can call the IIPS Help Desk for assistance.

VERIFY THAT SYSTEM GENERATED PASSWORDS HAVE CHANGED

The Reset Password feature is an example of how passwords are system generated. As in the current system, a user will receive an e-mail notification with their user name and new password. Included in the e-mail message is a hyperlink to the IIPS Login page. Once the user attempts to login with the new password, the user will be immediately redirected to the Change Password page.

SESSION-LOCK AFTER '3' INVALID ATTEMPTS

IIPS is now configured to monitor the login attempts of each user. After three (3) consecutive failed login attempts, the user's account will be locked out of the system for 30 minutes. With each login attempt, a new window will appear warning the user that the name and/or password

entered is incorrect. After the 30-minute waiting period, the account will be re-instated and the user can attempt to login again. The user can choose to reset their password; however, the user will not be able to login until after the 30-minute waiting period. If the user needs immediate assistance, they have the option to call the IIPS Help Desk.

PASSWORDS FOR INTERNAL USERS ONLY

Users who are a Contracting Officer, Contract Specialist, or Evaluator for the U.S. Department of Energy were notified in groups to update their passwords to meet the CIO Office's security requirements. Users who do not change their password within a specified time will have their access reduced.

GENERATIONS OF EXPIRED PASSWORDS

IIPS is now able to track up to 3 previously used passwords by any given user. While the passwords are tracked, they are also encrypted. Users must enter a different password each time they change their password.

UPGRADE IIPS SERVERS TO DOMINO 6.5X

In order to implement many of the security features, it was necessary to upgrade the IIPS servers to the new Domino 6.5x version. Once servers were upgraded, features and functions of IIPS were tested and validated.

PASSWORD AGING/EXPIRATION

Users are now required to change their password every 12 months from the last password change date. If a user has not changed their password for 12 months and attempts to login to IIPS, the user will be redirected to the Change Password Request page.

PASSWORD QUALITY LEVEL

When a user changes their password, it must meet a quality level of 12. To understand what that means, a link to "Password Quality Guidance" is available on the registration page. Helpful hints as well as examples of acceptable passwords are provided to assist the users.

ENHANCEMENTS

LOGIN

As an extra feature to IIPS, users can now view their last login information. When a user successfully enters their user name and password, a dialog box will appear with the user's last login date, time, and the appropriate IIPS system.

PASSWORD QUALITY STRENGTH

To assist the user with selecting a password that will meet security requirements, a new feature has been added. A link to "Test Your Password Strength" can be found in the "Password Help" box on the registration page and the "Password Change Request" page. Users can test as many passwords as they like before submitting their request.